https://doi.org/10.7840/kics.2023.48.8.992

머신러닝과 딥러닝을 이용한 텔레메트리 데이터 암호해독

안 주 언[◆°], 김 지 은[*], 이 택 준[*]

Cryptanalysis of Telemetry Data Using Machine Learning and Deep Learning

Joo-eon Ahn[◆°], Ji-eun Kim[*], Taek-joon Yi[*]

요 약

ICT 기술이 발전하면서 국방과 항공우주 분야에서도 더 많은 데이터를 주고받고 있다. 랜섬웨어나 해킹 위협으로부터 데이터와 시스템을 지키기 위해 암호 알고리즘을 사용하고 있는데 사업별로 다른 암호 알고리즘이나 암호키를 사용하면 암호 모듈의 복잡성 또한 크게 늘어나고 있다. 따라서 머신러닝과 딥러닝 알고리즘의 암호해독 성능 비교를 통해, 랜섬웨어를 탐지하고 암호 모듈 관리 효율성을 증가시킬 시스템에 도입할 알고리즘을 선정하고자 한다. 성능 비교 결과 데이터 프레임 수가 적을 경우에는 머신러닝 알고리즘이 대체로 높은 정확도를 보여주었지만, 데이터 프레임 수가 늘어날수록 정확도가 떨어지고 학습 시간이 오래 걸리게 되었다. 딥러닝의 경우 CNN은 정확도와 학습 시간이 준수하였고 데이터 프레임 수가 늘어나더라도 성능이 크게 떨어지지 않는 모습을 보여 가장 적합한 알고리즘으로 선정하였다.

키워드 : 암호해독, 머신러닝, 딥러닝, 텔레메트리
Key Words : Cryptanalysis, Machine Learning, Deep Learning, Telemetry

ABSTRACT

With the development of ICT technology, more data is being exchanged in the defense and aerospace fields. Cryptographic algorithms are being used to protect data and systems from hacking and ransomware, and the complexity of cryptographic modules is also greatly increased by using different cryptographic algorithms or encryption keys for each business. Therefore, through the comparison of cryptographic performance of machine learning and deep learning algorithms, we want to select algorithms to be introduced into systems that detect ransomware and increase cryptographic module management efficiency. Performance comparisons show that machine learning algorithms generally show high accuracy when the number of data frames is small, but the accuracy decreases as the number of data frames increases It took a long time to learn. For deep learning, CNN was selected as the most suitable algorithm. Because it complied with accuracy and learning time and showed that performance did not decrease significantly even if the number of data frame increased.

◆° First and Corresponding Author : Danam Systems R&D Center, Seoul National Science and Technology University Department of Industrial and Information System, llckybbang@naver.com, 정회원
* Danam Systems R&D Center, jekim01@danam.co.kr; itboy@danam.co.kr, 정회원
논문번호 : 202302-023-C-RN, Received February 3, 2023; Revised April 10, 2023; Accepted May 16, 2023

Ⅰ. 서 론

ICT 기술이 발전하면서 사회와 전 산업에서 Digital Transformation이 발생하였다. 군용 통신 분야에서도 전투 행위 중 발생되는 정보의 전달, 고속화, 보안, 신뢰성 등으로 인해 더 많은 데이터를 송수신하기 원하고 있다.[1]

ICT 기술이 발전하면서 더 많은 데이터를 송수신할 수 있지만, 해킹이나 랜섬웨어 등 사이버 공격에 대한 위협도 증가하고 있다. 특히 2021년에는 NFT 시장이 성장하면서 NFT를 탈취하려는 공격이 증가하였다. 또한 가상화폐를 사용하면서 탈중앙화 금융(DeFi)가 공격의 대상이 되어 피해 규모가 수천억 원에 이르기도 하였다. 2022년에는 러시아-우크라이나 전쟁으로 인해 물리적인 공격과 함께 사이버 공간에서도 전투가 발생하였는데, 러시아는 침공을 하기 전부터 악성코드 배포, DDoS 공격 등을 진행하였다. 침공 이후에는 군사적인 공격 전후로 사이버 공격을 적극 활용하였다. 이러한 사이버전에 양쪽 진형을 지지하는 세력이 해커그룹이 가세하면서 러시아, 우크라이나에서 다른 나라와 민간 기업으로 범위가 확대되고 있다.[2]

통신을 통해 전송되는 데이터가 늘어나는 만큼 관리가 필요한 데이터 또한 늘어나 보안의 중요성도 같이 증가하게 되었다. 이로 인해 각 사업별로 다양한 암호 알고리즘과 암호키를 사용하면서 암호화/복호화 하는데 필요한 암호 모듈 관리의 복잡성도 증가하여 업무 효율성이 떨어지게 되었다.

이러한 문제점들을 해결하기 위해 딥러닝을 이용한 암호해독 방법을 제시하고자 한다. 업무 효율성 향상과 랜섬웨어와 같은 사이버 공격으로 데이터와 시스템을 보호하기 위해, 딥러닝을 이용하여 암호화 여부를 확인할 수 있다. 딥러닝을 이용하여 랜섬웨어 방지를 위해 다양한 연구가 진행 중이다. 랜섬웨어 방지 이외에도 사용자의 트래픽 데이터를 학습하여 사용자의 비정상 행위를 탐지는 방식으로 랜섬웨어를 판단하는 연구도 이루어지고 있다.[3]

암호해독(Cryptanalysis) 분야는 공격 유형에 따라 암호 모방 공격(Cipher Emulation Attack), 식별 공격(Identification Attack), 키 복구 공격(Key Recovery)으로 구분된다. 암호 모방 공격은 암호화 또는 복호화 과정을 학습하여 암호문을 평문으로 복원하거나 평문을 암호문으로 복원하는 공격을 뜻한다. 식별 공격은 평문과 암호문을 학습하여 어떤 암호 알고리즘으로 암호화 하였는지 예측하는 공격을 말한다. 키 복구 공격은 평문과 암호문을 이용하여 암호키를 복구하는 공격이다. 본 논문에서는 식별 공격을 응용하여 어떤 암호 알고리즘을 통해 암호화가 되었는지 예측해보았다. 예측한 결과 학습되지 않은 암호 알고리즘인 경우 랜섬웨어와 같은 사이버 공격으로 데이터가 오염되었다고 판단할 수 있다. 오염되었다고 판단한 데이터의 경우 시스템과 격리시키고 시그니처 기반의 기법 등 기존의 랜섬웨어 탐지 방법으로 탐지한 후 암호 방식이 학습되지 않은 데이터인지 랜섬웨어인지 판단이 필요하다. 랜섬웨어로 판단될 경우 조치 정책에 따라 시행하여 사이버 공격으로 인한 피해를 최소화 시킬 수 있다.[4]

ICT 기술 등 컴퓨터의 성장은 다양한 분야에서 연구개발을 촉진시키고 있다. 특히 컴퓨팅 성능 증가로 머신러닝, 딥러닝의 연구가 활발하게 이루어지고 있다. 암호 알고리즘의 암호학적 취약성을 분석하는 암호해독 분야에서 머신러닝, 딥러닝과 같은 방법의 적용은 미비한 편이다. 기존에는 입력값의 변화에 따른 출력값의 변화를 이용하는 차분분석(Differential Cryptanalysis)이 주로 공격에 사용되었고 이러한 취약점을 방어할 수 있는 암호 알고리즘을 설계하고 있지만 다양한 변형 공격 방식이 존재해 아직까지도 암호분석에 사용되고 있다. 최근에는 딥러닝을 이용하여 암호해독을 진행한 방법이 유행하고 있다. 특히 2019년 A. Gohr의 신경망 구분자 논문 발표 이후 암호문에서 평문을 복원하는 방법을 다양하게 시도해보고 있다.[5,6]

본 연구에서는 머신러닝 알고리즘과 딥러닝을 이용하여 암호해독 분야의 식별공격을 응용하여 암호 방식을 예측해보고 성능을 비교하여 랜섬웨어로부터 데이터와 시스템을 보호하고 업무 효율성을 개선시키는 것이 목적이다. 모델 성능 비교 결과 CNN이 가장 우수한 것으로 나와 신경망 네트워크 설계 변경을 통해 암호 방식 예측 성능을 향상시켜보았다.

Ⅱ. 연구배경

본 논문에서 사용한 암호 알고리즘에 대한 간략 설명과 암호 학습에 사용한 알고리즘을 간략히 설명하고자 한다.

2.1 이론적 배경

2.1.1 암호 알고리즘

2.1.1.1 DES (Data Encryption Standard)

데이터 암호화 표준(Data Encryption Standard, DES)는 56 비트의 키를 가지는 대칭키 암호 방식이다.

블록 암호의 한 일종으로 미국 정부에서 암호 기술에 대한 필요성 증가로 인해 표준적인 암호 알고리즘을 개발하게 되었다. IBM에서 제안한 암호 알고리즘을 수정하여 국가 표준으로 채택하였다. 당시에는 암호키 크기가 충분했지만, 현재 향상된 컴퓨팅 성능으로 인해 전수조사를 통해 금방 키를 복원할 수 있기 때문에 사용되지는 않는다.

2.1.1.2 AES (Advanced Encryption Standard)

고급 암호화 표준으로 DES를 대체할 목적으로 미국 표준 기술 연구소에서 공모를 통해 선정하였다. 표준화 과정을 거치면서 5년동안 15개의 암호 알고리즘이 경쟁하였고, 최종적으로 Rijndael 암호 알고리즘을 채택하였다. 대칭키 방식의 암호 알고리즘으로 암호키가 56비트로 고정인 DES와 달리 128, 192, 256 비트의 암호키를 사용할 수 있다. 암호 표준으로 채택 이후, 높은 암호 성능으로 전세계적으로 널리 사용 중이다.

2.1.1.3 RC4

RC4 암호 알고리즘은 스트림암호 방식으로 블록암호인 DES, AES에 비해 암호 안전성 및 신뢰도와 응용범위가 떨어진다. 하지만 스트림암호는 암호화 속도와 구현 효율성에서 블록암호보다 뛰어나다는 장점을 가지고 있다. 이러한 스트림암호에서 대표적인 암호 알고리즘이 RC4이다. 특징으로는 네트워크 프로토콜에서 주로 사용하는데 구현이 쉽고 빠르다는 장점을 가지고 있다.

2.1.2 머신러닝 & 딥러닝

2.1.2.1 SVM(Support Vector Machine)

SVM은 백터 공간에서 데이터를 2개 그룹으로 구분짓는 선형 분리자를 찾는 모델이다. 백터 공간의 차원은 모델에 사용되는 데이터의 독립변수의 수다. 백터공간이 2차원이라면 선형 분리자는 직선이 되는데 식은 아래와 같다.

$$Y = w^T x + b \tag{1}$$

w는 직선에 수직인 법선 벡터이고 b값에 따라 직선이 평행 이동하게 된다. 즉 SVM은 직선을 움직이면서 최대한 2개의 그룹을 잘 구분할 수 있도록 하는 것이 핵심 개념이다. 그룹을 잘 구분하기 위해서는 두 그룹을 최대한 멀리 떨어진 직선식을 구해야 한다. 데이터가 새로 추가가 되어도 분류를 잘하기 위해서는 그룹 간 거리가 멀어야 한다. 선형 분리자와 가장 가까이 있는 데이터를 서포트 벡터라고 하는데 각 그룹의 서포트 벡터의 차이를 마진이라고 한다. 따라서 그룹 간 거리를 대표할 수 있는 마진을 최대화 시키는 방향으로 최적화 문제를 만들어 최적의 선형 분리자를 계산하는 방법이 SVM이다.

본 연구에서는 SVM을 적용하여 암호분석을 진행할 때 커널 트릭을 사용하였다. SVM은 데이터 구분을 선형으로 밖에 구분할 수 없기 때문에 XOR 문제같이 선형 분류가 어려운 데이터가 존재한다. 이를 해결하기 위해서 커널 트릭을 사용하는데 데이터를 선형으로 구분할 수 있는 차원으로 변환시키는 방법을 말한다. 네 종류의 커널 트릭을 사용하였고 각 성능을 비교하였다.

2.1.2.2 Naïve Bayes

베이즈 정리에 기반해서 만들어진 분류기로, 단순한 지도 학습 방법 중 하나이지만 대용량 데이터에 대해 빠른 속도와 높은 정확성을 가지는 것으로 알려져 있다. 베이즈 정리는 아래 식과 같다.

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \tag{2}$$

베이즈 정리는 사전확률과 사후확률의 관계를 정리한 식으로 분류기에 사용되는 모든 변수를 독립이라 가정하는 것이 가장 큰 특징이다.

2.1.2.3 CNN (Convolutional Neural Network)

사람의 시각인지 과정을 모방한 신경망으로 컴퓨터 비전 분야에서 탁월한 성능을 보이고 신호 처리나 음성 인식 등 다양한 분야에서 활용되고 있다. 합성곱(Convolution)을 신경망에 적용하여 데이터에서 특성을 추출하기 위해 필터를 사용한다. 필터와 규제화, 드롭아웃, 배치 정규화를 이용하여 데이터에서 특성을 보다 쉽게 추출이 가능하다. 즉 CNN은 전체 데이터에서 반복적으로 필터를 적용하여 특성을 추출하고, 이를 이용하여 패턴을 찾아 내는데 특화된 신경망이다.

2.1.2.4 LSTM

음악, 영상 등 연속적인 구조를 가지는 데이터 분석을 위한 신경망으로 순환구조를 가지는 것이 특징이다. 여기서 순환의 의미는 자기 자신을 참조하는 것으로 현재 나타난 결과가 이전의 결과에 의해 나타났다는 의미이다. 순환 신경망인 RNN이 가진 가중치가 업데이트 되면서 1보다 작은 값을 계속 곱하기 때문에 기울기 소멸 문제가 발생한다. 이를 해결하기 위해 RNN을 변

형해서 LSTM이나 GRU와 같은 신경망을 사용한다. 기울기 소멸 문제를 해결하기 위해 LSTM은 4개의 Layer와 Cell을 추가해 상태를 설정하여 장기 기억, 단기 기억으로 나누고 기억할 정보와 잊을 정보를 선택하여 시계열 처리가 가능한 신경망이다.

2.2 선행연구

A. Gohr이 암호해독 분야 중 키 복구 공격에 딥러닝 기술을 이용하여 경량 블록암호 분석을 제안하면서 암호 학계에서도 딥러닝에 관심을 가지게 된 계기가 된다. 기존에는 차분분석을 활용하여 키 복구 공격을 하는 방식이 주로 사용되었다. 신경망이 차분분석 방법을 보완하면서 관련 연구들이 등장하기 시작했다. 신경망을 이용한 차분공격은 암호문이 가지고 있는 차분특성을 학습하는 것이 핵심이다. A. Gohr의 신경망 구분자 연구를 토대로 여러 시험을 진행하여 Speck32/64와 비슷한 암호 방식인 Simon32/64도 신경망을 통해 복호화가 가능함을 보여주었다.[7]

DES 암호 알고리즘과 ECB(Electronic Codebook) 모드를 사용하여 암호화된 암호문과 평문 쌍을 신경망을 통해 암호키 없이 복호화 시도를 통해 신경망의 근사 가능성을 보여주었다.[8] 하지만 평문과 암호문 쌍을 만들어 신경망을 이용하여 실제로 예측해본 결과, 신뢰성이 떨어진다는 결과도 있다.[9]

신경망을 이용하여 평문 복원의 가능성을 검증하기 위한 연구도 진행되었다. 암호 분석에서 기존에 차분특성을 이용하여 키 복구 공격이 일반적이었다. 반면 최근에 진행되고 있는 신경망 기반 평문 복구 공격은 복호화 알고리즘에 근사하는 방법이다. 신경망의 근사 특성상 연속함수를 근사할 때는 효율적인 반면 이산함수를 효율적으로 근사하는 연구 결과는 찾아보기 힘들다. 따라서 평문 복구 공격 연구를 위해 신경망이 연속함수와 이산함수 모두 근사 가능한지 실험을 진행하였다. 연속함수의 경우 알려진 근사 특성에 따라 잘 학습되고 있음을 확인한 반면 이산함수의 경우 신경망으로 잘 학습되지 않는 점을 확인하였다. 이러한 특성으로 신경망을 이용하여 평문을 복원하는 것은 어려움이 있는 것으로 보인다.[10]

또한 랜섬웨어 방어를 위해 신경망을 사용한 연구도 있다. 기존에 랜섬웨어 탐지 방식은 공격 기법을 미리 알고 있는 상태에서 이를 탐지하는 시그니처 기반의 탐지 방법이 주로 사용되어 왔다. 시그니처 기반의 탐지 방법의 문제점은 알지 못하는 패턴으로 공격이 들어올 경우 대처하기 힘들다는 점이다. 이러한 한계점을 개선하기위해 여러 연구들이 진행되어 왔는데 그 중에 하나가 딥러닝을 이용한 방법이다. 랜섬웨어는 다양한 암호 방식으로 암호화가 진행이 되기 때문에 어떤 암호 알고리즘으로 암호화가 되었는지 판단하는 것이 중요하다. 이를 판단하기 위해 DES, AES, RSA 등 여러 암호 알고리즘으로 암호화가 된 데이터를 이용하여 해당 데이터가 암호화된 데이터인지 판단하여 93.90%의 정확도로 판단이 가능하였다.[11]

해외에서는 주로 A. Gohr의 신경망 구분자를 더욱 발전시키는 연구를 진행중이다. 주로 신경망 입력 데이터로 평문과 암호문 쌍을 이용하여 차분특성을 파악한 뒤 테이블로 구성하게 된다. 이를 신경망 모델에 학습시켜 Key 예측 성능을 향상시키고 있다. A. Gohr가 시도했던 것처럼 성능 개선에 경량블록암호를 이용하는데 연구마다 조금의 차이는 있지만 주로 SPECK32/64, SIMON32/64, GIFT를 사용하고 있으며, 암호화 알고리즘 종류를 늘려가는 중이다. 또한 데이터의 복잡도와 암호 Round를 기존보다 개선시키면서 신경망 구분자의 Key 예측 성능을 향상시키고 있다.[12-15]

암호해독 분야 중 암호화나 복호화 방식을 학습하는 암호 모방 공격의 성능을 개선시키는 연구도 진행중이다. 이 연구들도 대부분 경량블록암호를 대상으로 연구를 진행중이다. 평문을 이용하여 암호문을 복원하거나 암호문을 이용하여 평문을 복원하고 있다. 추가적으로 DES 암호 알고리즘을 간소화하여 사용하는 S-DES도 연구하고 있다. DES 알고리즘을 사용한 암호문을 64bits 단위로 학습하여 평문으로 복원한 결과, 최대 97%에 달하는 정확도를 보여주며 암호 모방 공격에서도 신경망이 유용하게 사용될 수 있음을 보여주었다.[16,17]

본 연구에서는 텔레메트리 계측 데이터를 DES-ECB, AES-CBC, RC4 암호 알고리즘을 이용하여 암호화를 진행하고 신경망을 통해 이를 구분해보고자 한다. 선행연구 사례를 통해 아직까지 신경망을 이용하여 평문을 복원하는 공격은 경량블록암호를 사용해야하는 한계점이 있는 것으로 보인다. 텔레메트리 데이터를 설계할 때 암호화 방식은 미리 협의를 하고 개발을 진행하기 때문에 암호화 방식만 알면 데이터 복호화가 가능하다. 따라서 신경망을 이용해 어떤 암호 알고리즘으로 암호화가 되었는지 판단하여 기존에 알고 있던 암호 알고리즘이 아니라면 랜섬웨어일 가능성이 있어 사전에 데이터를 격리하여 다른 데이터와 시스템을 보호할 수 있다. 시스템으로 암호화 종류를 판단하면 여러 암호 알고리즘을 관리하여 업무 효율성이 떨어지는 점을 개선할 수 있을 것으로 보인다.

Ⅲ. 연구방법

3.1 데이터 수집

암호해독에 사용된 데이터는 실제 시험 상태가 아닌 텔레메트리 데이터를 사용했다. 텔레메트리 안에는 각종 센서 데이터들이 할당되어 있다. 따라서 할당된 파라미터 값의 변화가 크지 않거나 동일할 수도 있다. 암호 알고리즘에 따라 엔트로피 특성을 이용하여 딥러닝 분류 성능을 비교하였다. 아래 그림과 같이 수집한 데이터는 총 5,000 프레임으로 암호화가 되지 않은 원본 데이터이다. 따라서 DES, AES, RC4 암호 알고리즘을 이용하여 암호화를 진행하였고, 총 20,000 프레임 데이터를 구성하여 학습데이터로 사용하였다. 테스트 데이터도 마찬가지로 5,000 프레임의 텔레메트리 데이터를 획득하였고, 각 암호 알고리즘으로 암호화를 하여 총 20,000 프레임 데이터로 구성하였다. 각 데이터 개수 별 모델의 강건성을 시험하기 위해 1,000 프레임 씩 데이터를 학습하여 총 4,000개의 데이터 성능과 5,000 프레임 씩 총 20,000 프레임 성능 시험을 나누어서 진행하고 비교하였다.

사용한 암호 알고리즘으로는 DES의 경우 ECB 암호 모드를 사용하였고 AES는 CBC 암호 모드를 사용하여 데이터를 생성하였다.

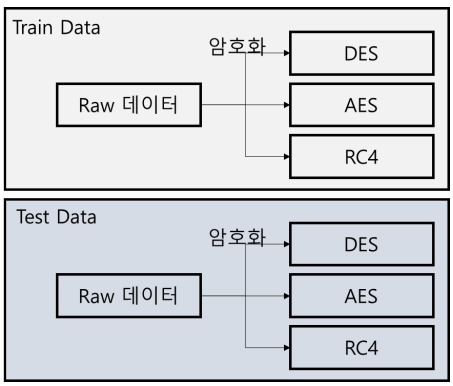


그림 1. 데이터 수집 절차
Fig. 1. Data Collection Procedure

3.2 데이터 분석

암호 해독 절차는 아래와 같다.

수집한 데이터에서 Sync 패턴을 찾아 프레임으로 구성한 뒤에 각 암호 알고리즘으로 암호화를 진행해 학습데이터와 시험 데이터를 만들었다. 한 프레임은 Sync Pattern을 제외하고 총 2048 Bytes로 구성하였고, 채널 데이터가 Word단위로 할당되어 있기 때문에 16Bits씩

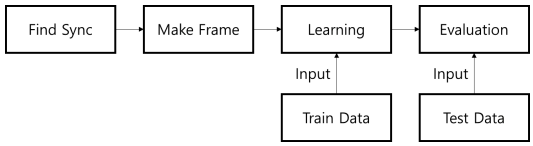


그림 2. 암호 해독 절차
Fig. 2. Decryption Procedure

할당하여 입력데이터를 구성하였다. 따라서 독립변수는 1024개의 채널로 구성되었고 종속 변수의 설정은 아래 표와 같다.

표 1. 종속변수
Table 1. Dependent Variable

Variable Values	Variable Types
0	Raw Data
1	DES Data
2	AES Data
3	RC4 Data

이러한 데이터를 이용하여 SVM, Naïve Bayes, CNN, LSTM 모델을 이용하여 암호를 분류해 보았다.

SVM은 커널 종류를 변경하며 암호 해독 성능을 평가했으며, Naïve Bayes는 1024 채널의 독립을 가정하고 성능 평가를 진행하였다. 머신러닝은 Python의 사이킷런(sklearn)을 사용하여 분석을 진행했다.

딥러닝은 CNN, LSTM을 진행하였는데 신경망 설계에 따라 성능에 많은 차이를 보였다. CNN의 경우 은닉층에 뉴런이 많을수록 최적화가 쉬워지고 Depth가 깊을수록 성능이 높은 것으로 알려져 있어 Layer를 추가하며 성능 평가를 진행하였다. LSTM의 경우 LSTM 층이 많을수록 성능이 떨어지는 경향이 있어 LSTM층과 완전연결망층만 추가하고 뉴런의 수만 조절하여 성능 평가를 진행하였다. 실제 구현은 Python의 Tensorflow2.0 Keras를 이용하여 진행하였다. 상세 신경망 설정은 아래와 같다.

A. Gohr의 신경망 구분자나 성능을 개선한 신경망 모델의 경우 CNN을 사용하였으며 신경망 Layer 사이에 Batch Normalization을 사용하면 신경망의 예측 성능이 좋아지는 것으로 알려져 있다. 본 연구에서도 Batch Normalization의 사용 여부에 따라 예측성능에 큰 차이를 보여주었다. Conv1D와 Dense Layer에서 활성함수로는 "Relu"를 사용하였고 최종 출력 Dense Layer에서는 "Softmax"를 사용하였는데 일반적인 신경망 구분자 모델에서는 "Sigmoid"를 사용하는 것이 일반적이나 암호방식을 구분할 때에는 "Softmax"가 높

표 2. 신경망 구조
Table 2. Neural Networks Structure

Neural Networks	Layer
CNN	Conv1D(1024)-Batch Normalization-Conv1D (512)- Batch Normalization-Conv1D (256)- Batch Normalization-Conv1D (128)- Batch Normalization-Flatten-Desne(128)-Desne(64)-dropout(0.5)- Desne(4)
LSTM	LSTM(1024)-Dense(128)-Dense(4)

은 성능을 보여주었다.

그 결과 SVM, Naïve Bayes와 같은 머신러닝 알고리즘들이 정확도 면에서는 높았지만 학습 데이터가 늘어날수록 학습시간이 기하급수적으로 늘어나는 현상을 보였고 성능이 크게 저하되는 알고리즘도 있었다. 따라서 CNN이 학습 속도, 정확도 면에서 뛰어난 성능을 보여주어 CNN을 기반으로 암호 분류 정확도를 높여 나갔다.

Ⅳ. 연구 결과

4.1 SVM 결과

SVM은 커널 변환에 따라 큰 성능 차이를 보인다. 딥러닝 등장 이전에 널리 사용되었던 알고리즘이라 관련 연구가 많은데 그로 인해 다양한 커널이 등장하였다. 커널 함수를 변경하여 총 4가지 커널 함수를 비교하며 적용하였고 그 결과는 아래와 같다.

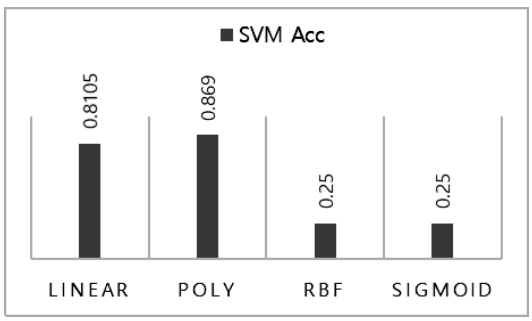


그림 3. SVM 결과
Fig. 3. SVM Result

커널 함수는 Linear, Poly, RBF, Sigmoid로 총 4가지 함수를 이용하여 분석을 진행하였고 정확도는 Poly 커널 함수가 가장 높은 것으로 나타났다. RBF, Sigmoid의 경우 무작위로 선택하는 확률인 0.25로 나와 암호 해독 성능은 크게 떨어지는 것으로 나왔다.

4.2 Naïve Bayes 결과

Naïve Bayes의 경우 각 변수들을 독립이라 가정하여 분류를 한다는 점이 가장 큰 특징이다. 즉 1024 채널이 모두 독립적이라고 가정하고 분석을 진행하게 된다. Naïve Bayes의 경우 1,000개씩 데이터 프레임을 사용하여 총 4,000개의 데이터 프레임으로 암호해독을 진행할 경우 0.8295로 높은 정확도를 보여줬으나 5,000개씩 총 20,000개 데이터 프레임으로 데이터 개수를 늘릴 경우 성능이 다소 떨어지는 것으로 보아 데이터 개수가 늘어날수록 성능이 떨어질 가능성이 있어 보인다. 하지만 본 연구에서 비교한 모델 중 가장 좋은 성능을 보여주기 때문에 향후 연구에서 모델 성능 기준으로 사용하거나, 빠른 검사를 요구하여 표본 검사 기능을 개발할 때 사용이 가능할 것으로 보인다. 예를 들어 텔레메트리 데이터 중 표본을 추출하여, 해당 모델을 사용하면 빠르게 암호 알고리즘을 판별할 수 있다.

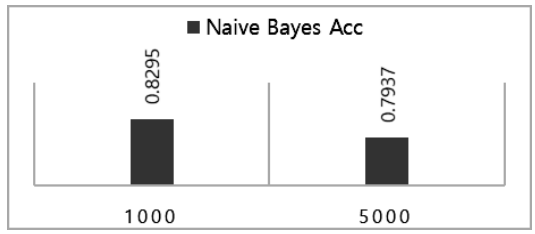


그림 4. Naïve Bayes 결과
Fig. 4. Naïve Bayes Result

4.3 CNN 결과

CNN은 신경망 구성에 따라 성능에 많은 차이를 보여준다. 앞서 설계한 신경망을 기준으로 1,000개씩 총 4,000개 데이터 프레임과 5,000개씩 총 20,000개의 데이터 프레임으로 CNN의 암호 해독 성능을 분석하였다.

성능 평가 결과 CNN의 경우 데이터의 개수가 늘어나도 성능에 큰 변화는 없어 모델의 강건성을 잘 보여주고 있다. 실제 시험 시간에 따라 편차는 존재하지만, 본 연구에서 시험으로 사용한 데이터 프레임보다 수가 많을 것으로 예상된다. 따라서 데이터 수가 증가하더라도 정확도를 꾸준히 유지하는 것은 모델을 선택할 때, 중요한 지표가 될 수 있다.

또한 해외나 국내에서 신경망 구분자 모델을 설계할 때 사용하고 있는 모델이기 때문에 앞으로 성능 개선할 수 있는 여지가 많다. 향후 연구에서 성능 개선을 하고자 할 때, 신경망 네트워크 구조를 변화시켜가며 성능을 향상시킬 수 있는 가능성이 있는 모델이다

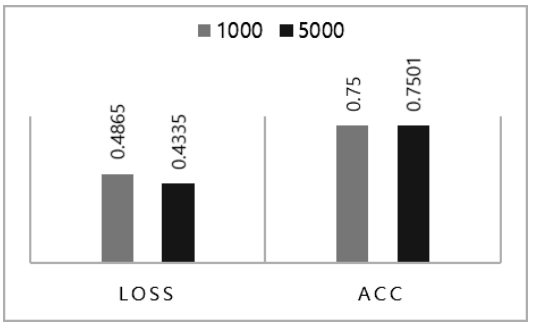


그림 5. CNN 결과
Fig. 5. CNN Result

4.4 LSTM 결과

LSTM은 텔레메트리 데이터가 시계열적 특성을 가지고 있어 높은 성능이 나올 것이라 기대했다. 하지만 암호화 진행 시 데이터가 가지고 있는 시계열 특성이 사라지기 때문에 LSTM을 사용하여 예측하는 것이 의미가 없어진다. 아래 그림과 같이 정확도가 0.25가 나와 무작위로 선택하는 확률과 동일한 확률이 나와 암호 해독 모델로 선택할 가능성이 낮다.

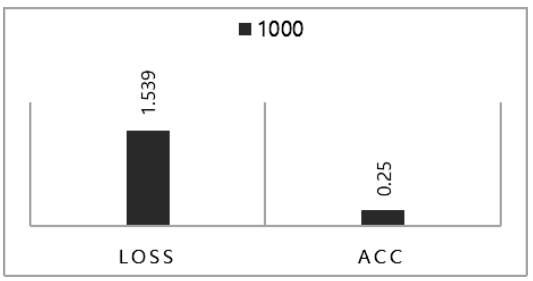


그림 6. LSTM 결과
Fig. 6. LSTM Result

V. 결 론

본 연구는 암호화된 텔레메트리 데이터의 랜섬웨어 사전 탐지 및 암호 모듈 관리 효율성 증가를 위한 시스템의 사전 연구로 암호 해독 성능을 비교해 보았다. 적은 양의 데이터 프레임의 암호 해독을 진행할 경우 머신러닝 알고리즘들이 뛰어난 성능을 보여주었다. 하지만 데이터 프레임의 수가 늘어날수록 성능은 떨어지고 학습시간마저 기하급수적으로 늘어난다는 단점을 가지고 있었다. 다만 Naïve Bayes 모델은 본 연구에서 뛰어난 성능을 보여주었기 때문에 향후 연구에서 성능 개선의 기준으로 삼거나, 빠른 시간 내에 검사가 필요할 경우 표본 검사 모델로서 사용이 가능할 것으로 보인다. 딥러닝의 경우 텔레메트리 데이터 중에 시계열적인 요소를 가지고 있는 채널이 있어 LSTM이 뛰어난 성능을 가지고 있을 것이란 예상과 달리 암호화로 인해 시계열이 특성이 없어짐으로 CNN이 암호 해독 시에 더 높은 성능을 보여주었다. CNN은 국내와 해외에서 신경망 구분자 모델로 선택하여 많은 연구가 진행중이기 때문에 향후 CNN을 기반으로 암호 해독을 진행한다면 더욱 높은 성능을 보여줄 수 있을 것으로 기대된다.

References

[1] D. H. Min, Y. H. Shin, and J. Y. Ahn, "[Insight Report] Wired networks: Focused on intelligence and optical networks," *ETRI Insight*, Jun. 28, 2019. from http://doi.org/10.22648/ETRI.2019.B.000027.

[2] KISA, "*Cyber Threat Trends Report in the first half of 2022*," Jul. 25, 2022, from https://www.kisa.or.kr/20205/form?postSeq=1022&lang_type=KO&page=1#fnPostAttachDownload.

[3] Y. S Lee, H. J. Choi, D. M. Shin, and J. J. Lee, "Deep learning based user anomaly detection performance evaluation to prevent ransomware," *J. SAV*, vol. 15, no. 2, pp. 43-50, Dec. 2019. (http://dx.doi.org/10.29056/jsav.2019.12.06)

[4] B. Seok and C. Lee, "Neural network decryption research trend analysis for block cipher," *The Korea Inst. Inf. Secur. and Cryptology*, vol. 31, no. 6, pp. 19-29, Jun. 2021.

[5] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptology*, vol. 4, pp. 3-72, Apr. 1991. (https://doi.org/10.1007/BF00630563)

[6] E. Jo, S. G. Kim, D. Hong, J. Sung, and S. Hong, "The statistical analysis of differential probability using GPGPU technology," *J. The KIISC*, vol. 29, no. 3, pp. 477-489, Mar. 2019. (http://doi.org/10.13089/JKIISC.2019.29.3.477)

[7] H. Seong, H. Yoo, Y. Yeom, and J. S. Kang, "Analysis of Gohr's neural distinguisher on speck32/64 and its application to simon32/64," *J. The KIISC*, vol. 32, no. 2, pp. 391-404,

Feb. 2022.
(http://doi.org/10.13089/JKIISC.2022.32.2.391)

[8] S. Fan and Y. Zhan, "Analysis of des plaintext recovery based on bp neural network," *Secur. and Commun. Netw.*, pp. 1-5, 2019.
(https://doi.org/10.1155/2019/9580862)

[9] S. Kwon, H. Yim, J. Kang, and Y. Yeom, "A study on the cryptanalysis of DES using neural network," in *Proc. KICS ICC 2020*, pp. 577-578, YongPyong, Korea, Aug. 2020.

[10] S. Kwon, H. Yim, J. Kang, and Y. Yeom, "Revisiting cryptanalysis of neural plaintext recovery attack of DES" *J. KICS*, vol. 46, no. 7, pp. 1109-1119, Jul. 2021.
(https://doi.org/10.7840/kics.2021.46.7.1109)

[11] M. Kang, J. Won, J. Park, and J. Kim, "A CNN-Based encrypted data detection for ransomware defense," *KIISE Trans. Comput. Practices*, vol. 25, no. 5, pp. 279-283, May 2019.
(https://doi.org/10.5626/KTCP.2019.25.5.279)

[12] Z. Hou, J. Ren, and S. Chen, "Cryptanalysis of round-reduced SIMON32 based on deep learning," *Cryptology ePrint Archive*, 2021.
(https://eprint.iacr.org/2021/362)

[13] T. Yadav and M. Kumar, "Differential-ML distinguisher: Machine learning based generic extension for differential cryptanalysis," *Progress in Cryptology – LATINCRYPT 2021*, vol. 12912, pp. 191-212, Springer, 2021.
(https://doi.org/10.1007/978-3-030-88238-9_10)

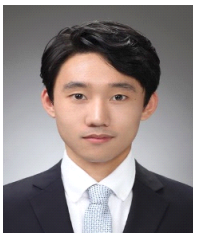
[14] A. Benamira, D. Gerault, T. Peyrin, and Q. Q. Tan, "A deeper look at machine learning-based cryptanalysis," *EUROCRYPT 2021*, vol. 12696, pp. 805-835, Springer, 2021.
(https://doi.org/10.1007/978-3-030-77870-5_28)

[15] Z. Bao, J. Guo, M. Liu, L. Ma, and Y. Tu, "Enhancing differential-neural cryptanalysis," *ASIACRYPT 2022*, vol. 13791, pp. 318-347, Springer, 2022.
(https://doi.org/10.1007/978-3-031-22963-3_11)

[16] S. Andonov, J. Dobreva, L. Lumburovska, S. Pavlov, V. Dimitrova, and A. Popovska-Mitrovikj, "Application of machine learning in DES cryptanalysis," *Progress in ICT Innovations 2020*, pp. 1-11, ISSN 1857-7288, 2020.

[17] J. So, "Deep learning-based cryptanalysis of lightweight block ciphers," *Security and Communication Networks*, vol. 2020, pp. 1-11, 2020.
(https://doi.org/10.1155/2020/3701067)

안 주 언 (Joo-eon Ahn)

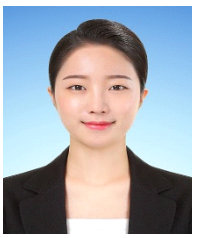


2017년 8월 : 서울과학기술대학교 산업공학 석사
2017년 7월~2023년 4월 : 단암시스템즈 선임연구원
2019년 3월~현재 : 서울과학기술대학교 산업공학 박사과정

<관심분야> 머신러닝, 딥러닝, 텍스트마이닝, 산업공학

[ORCID:0000-0001-7088-6247]

김 지 은 (Ji-eun Kim)



2020년~현재 : 단암시스템즈 연구원

<관심분야> 머신러닝, 딥러닝, 프로세스마이닝, 산업공학

[ORCID:0009-0004-4632-0074]

이 택 준 (Taek-joon Yi)

2004년 8월 : 충북대학교 전자계산학 석사

2005년 3월~현재 : 단암시스템즈 수석연구원

<관심분야> 컴퓨터과학, 통신공학, 텔레메트리, 인공지능

[ORCID:0000-0001-8525-623X]